

CLAIMS

1. Method for creating and managing a local network, this network comprising at least one restitution device for an encrypted data stream and a diffusion and re-encrypting device for all or part of said encrypted data, said devices comprising security modules, the method comprising the following steps:
 - connecting a master security module in one of the devices connected to the local network,
 - establishing a network key by the master security module,
 - securely transmitting this network key to one or several user security modules,
 - decrypting encrypted data by the diffusion and re-encrypting device,
 - re-encrypting of the data by said device with a local key,
 - transmitting the re-encrypted data to the restitution device,
 - decrypting by said restitution device thanks to the associated user security module, which disposes of means to find the local key.
2. Method for creating and managing a local network according to claim 1, wherein the local key is a randomly generated session key encrypted by the network key.
3. Method for creating and managing a local network according to claim 1, wherein the local key is the network key.
4. Method for creating and managing a local network according to claim 1, wherein the establishment of the network key is obtained by the pseudo-random generation of a key during the initialization of the local network.
5. Method for creating and managing a local network according to claim 1, wherein the establishment of the network key is carried out during an initialization step of the master module.
6. Method for creating and managing a local network according to claim 1, wherein the master module is placed in a removable security module.
7. Method for creating and managing a local network according to claim 6, wherein said removable security module comprises a user module forming part of the network administrated by the master module.

8. Method for creating and managing a local network according to claim 1, wherein the user security modules are in the form of an electronic circuit mounted during the manufacture of the restitution device.
9. Method for creating and managing a local network according to claim 1, wherein the user security module is in the form of a removable security module.
10. Method for creating and managing a local network according to claim 1, wherein the diffusion and re-encrypting device includes a security module, called converter module, said module receives and keeps an identifier of the master module that created the network, the converter module re-encrypting the data for said network.
11. Method for creating and managing a local network according to claim 10, wherein said master module identifier is transmitted to a management center during a connection step to said management center.